IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION

UNITED STATES OF AMERICA	**PLAINTIFF**
V.	**CAUSE NO. 3:17-cr-77-CWR-LRA**
NIKOLAOS T. KOUTSOS, et al.	**DEFENDANTS**

ORDER

Before the Court is Lai Saechao's Second Motion to Suppress. After considering the briefs, applicable law, and arguments presented at a hearing held this day, the Motion will be denied.

I. Background

Nikolaos Koutsos, James Horrisberger, and Lai Saechao were arrested and charged with possession of marijuana with intent to distribute, conspiracy to possess marijuana with intent to distribute, and interstate transportation in aid of racketeering. Horrisberger and Saechao first moved to suppress the marijuana seized in connection to their detention and arrest. That motion was denied, *see United States v. Koutsos*, 3:17-CR-77-CWR-LRA, 2017 WL 5615893, at *7 (S.D. Miss. Nov. 21, 2017), as was their motion for reconsideration, *see United States v. Koutsos*, 3:17-CR-77-CWR-LRA, 2018 WL 523944, at *5 (S.D. Miss. Jan. 23, 2018).

Saechao now moves to suppress the material the government found on his electronic devices, particularly his Samsung Galaxy Note. These devices (and others) were seized upon Defendants' arrest on June 6, 2017.[1] On June 30, 2017, the government applied for and obtained search warrants to download and analyze material from the devices. The warrants expired on

[1] Homeland Security agents found the Samsung phone on the Piper airplane, not on Saechao's person. For this motion only, Saechao presumes that he has a legitimate expectation of privacy in the phone's contents pursuant to the Fourth Amendment. Therefore, standing is not contested.

July 12, 2017. Two days later, however, the government extracted data from Saechao's Samsung Galaxy Note.

II. Legal Standard

The Fourth Amendment protects against unreasonable searches and seizures, but "says nothing about suppressing evidence obtained in violation of this command." *Davis v. United States*, 131 S. Ct. 2419, 2426 (2011). Rather, the exclusionary rule is a prudential doctrine created by the Supreme Court to "compel respect for [the] constitutional guaranty." *Id*. "The rule's sole purpose . . . is to deter future Fourth Amendment violations." *Id*. (citations omitted).

III. Discussion

Saechao challenges the search warrants on three grounds. Each will be discussed in turn.

A. Expired Search Warrants

Saechao first contends that evidence from his devices should be suppressed because it was obtained two days after the government's warrants expired.

When a warrant authorizes a search for electronically stored information, "officers may (1) seize or copy the entire storage medium and (2) review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41 advisory committee's note to 2009 amendment. The first step, the execution period, is limited to a "specified time no longer than 14 days." Fed. R. Crim. P. 41(e)(2)(A). The second step, the review period, is unlimited unless otherwise specified by the magistrate. "A substantial amount of time can be involved in the forensic imaging and review of information." Fed. R. Crim. P. 41 advisory committee notes to 2009 amendment.

In this case, each warrant commanded officers "to execute this warrant on or before July 12, 2017." The deadline of July 12 "refer[red] to the seizure or on-site copying of the media or

information, and *not* to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B). The government missed this deadline. The government seized Saechao's cell phone well before July 12, 2017, but it failed to seize or extract the media until two days later.

Although the government did not satisfy the warrant's time requirements, its conduct does not necessarily result in suppression. In *United States v. Chambers*, officers executed a search warrant two days after it expired. No. 1:07-CR-15, 2007 WL 287406, at *1 (S.D. Miss. Sept. 27, 2007). Despite this delay, Judge Guirola denied the defendant's motion to suppress for the following reasons: (1) there was "no showing that the delay was the result of intentional disregard of the warrant terms"; (2) the warrants were executed within the 10-day requirement of Rule 41";[2] and (3) there was "no showing that probable cause was affected by the passage of slightly more than two days beyond the warrant issue date." *Id.*

The Fifth Circuit has not directly addressed this issue, but generally applies the following standard for Rule 41 violations:

> Unless a clear constitutional violation occurs, noncompliance with Rule 41 requires suppression of evidence only where, (1) there was *prejudice* in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of *intentional and deliberate disregard* of a provision in the Rule.

United States v. Comstock, 805 F.2d 1194, 1205 (5th Cir. 1985) (emphasis added).[3]

Here, Saechao does not argue that the two-day delay prejudiced him in any way, and there is no record evidence that the government intentionally or deliberately disregarded Rule 41(e)(2). The two-day delay does not require suppression.

[2] In 2009, the time set in the former rule at 10 days was revised to 14 days. *See* Fed. R. Crim. P. 41 advisory committee's note to 2009 amendment.

[3] Other federal courts have held that a minor, unintentional, and non-prejudicial delay in executing a warrant does not require suppression. *See United States v. Sims*, 428 F.3d 945, 955 (10th Cir. 2005); *United States v. Gerber*, 994 F.2d 1556, 1560 (11th Cir. 1993).

B. General Search

Saechao next argues that the government's lack of a search method converted the warrants into "general warrants" long held to be unconstitutional. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

The Fourth Amendment prohibits search warrants that permit "a general, exploratory rummaging in a person's belongings." *Williams v. Kunze*, 806 F.2d 594, 598 (5th Cir. 1986) (citation omitted). The description in the warrant must use "sufficient particularity such that the executing officer is left with no discretion to decide what may be seized." *Id*. Where particularity is impossible, "generic language suffices if it particularizes the types of items to be seized." *Id*. Reasonable specificity is required; elaborate detail is not. *United States v. Triplett*, 684 F.3d 500, 504 (5th Cir. 2012).

Saechao presents a modern twist on this longstanding law. He does not argue that the warrant applications were insufficiently particular under the Fourth Amendment.[4] Rather, he challenges the warrant's failure to specify the *method* by which the government would have to conduct the search of gigabytes of electronically stored information. The government's brief misses this point.

Saechao contends that the "warrants should have included directions for how the government intended to conduct its search in such a way as to minimize its intrusion into information not covered by the warrant." Instead, he observes, the government performed "a wholesale download of all of the content of [his devices]," including emails dating back to 2009;

[4] When viewed alongside the supporting affidavit, the warrants issued in this case were "reasonably focused." *See Triplett*, 684 F.3d at 505 ("The law permits an affidavit incorporated by reference to amplify particularity, notwithstanding that, by its terms, the Fourth Amendment requires particularity in the warrant, not in the supporting documents."). Each warrant lists the specific model and serial number, if known, of the subject device. In the affidavit, the government requests authorization to search the devices for any text messages, contacts, flight logs, videos, and photos that are "evidence relevant to an ongoing multi-state, international criminal investigation involving the production, transportation, and distribution of marijuana."

telephone calls dating back to 2013; location data dating back to 2013; and pictures of family members, including children. Saechao relies on a case from the District of Kansas in which a magistrate judge denied a search warrant application because the court desired "a sophisticated technical explanation of how the government intends to conduct the search" of the defendant's cell phones. *In re Cellular Telephones*, No. L4-MJ-8017-DJW, 2014 WL 7793690, at *8 (D. Kan. Dec. 30, 2014). As the Sixth Circuit notes,

> [a] warrant may permit only the search of particularly described places and only particularly described things may be seized. As the description of such places and things become more general, the method by which the search is executed comes more important—the search method must be tailored to meet allowed ends.

United States v. Richards, 659 F.3d 527, 539 (6th Cir. 2011) (citation omitted).

The Court recognizes the difficulty, and increasing ubiquity, of the situation. Our electronic devices are now repositories of our whole lives, personal and professional, innocuous and criminal, for better or for worse. *See Riley v. California*, 134 S.Ct. 2473, 2489-90 (2014). Obviously, law enforcement officers should limit their exposure to irrelevant personal files on electronic devices.[5] *Triplett*, 684 F.3d at 506. And perhaps for that reason, it will become standard operating procedure for magistrate judges to place some basic guiderails on how electronically stored information may be searched.

Still, when searching an electronic device, "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders." *Triplett*, 684 F.3d at 506 (quotation marks and citation omitted). Federal courts

[5] In *United States v. Carey*, the Tenth Circuit suggested methods to avoid searching files not identified in the warrant, such as "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." 172 F.3d 1268, 1276 (10th Cir. 1999). Later, in *United States v. Burgess*, the Tenth Circuit offered the following guidance: "officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant." 576 F.3d 1078, 1092 (10th Cir. 2009).

have therefore applied a fact-specific reasonableness analysis to these situations, ultimately rejecting most particularity challenges to warrants which authorized the seizure and search of entire computers or devices. *See Richards*, 659 F.3d at 540-41 (collecting cases). For example, in *United States v. Summage*, the Eighth Circuit found that a warrant authorizing a broad search of a personal computer for child pornography was reasonable where, at the time the warrant was sought, "the officers knew only that a video and photographs of the alleged incident supposedly existed, not the particular format in which these items were being kept." 481 F.3d 1075, 1079 (8th Cir. 2007).

Such an analysis in this case leads to the same conclusion. The Court is not persuaded that a warrant has to provide directions for how to search electronically search information on a cell phone.[6]

C. Lack of Probable Cause

As an alternative argument, Saechao claims that the supporting "affidavit [did not] establish probable cause that evidence would be found on Saechao's devices." He argues that the affidavit was based not on "facts and circumstances" but merely on "belief or suspicion." *Nathanson v. United States*, 290 U.S. 41, 47 (1933). The Court disagrees.

This Court must afford "great deference" to a magistrate's determination of probable cause. *United States v. Allen*, 625 F.3d 830, 840 (5th Cir. 2010) (citation omitted). Probable cause to support a search warrant does not require proof beyond a reasonable doubt. *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007). "A magistrate needs only a substantial basis for concluding that a search would uncover evidence of wrongdoing." *Allen*, 625 F.3d at 840.

[6] Based on this Court's research, the Fifth Circuit does not require warrants to contain a particularized computer search strategy.

Here, the supporting affidavit sets forth the facts surrounding Saechao's arrest, which among other things involved the discovery of approximately 248 pounds of marijuana. The affiant, Agent McMillin, explains that, through his law enforcement training, knowledge, and experience with drug trafficking, drug traffickers often communicate about their business through cell phones. The totality of the circumstances supports that probable cause existed to search Saechao's cell phone.

IV. Conclusion

The Second Motion to Suppress is denied.

SO ORDERED, this the 27th day of March, 2018.

s/ Carlton W. Reeves
UNITED STATES DISTRICT JUDGE